UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

UNITED STATES OF AMERICA,	**)**	
	)	
Plaintiff,	**)**	
	)	
vs.	**)**	**Case No. 4:16CR00374 JAR/PLC**
	)	
ROLAND HOEFFENER,	**)**	
	)	
Defendant.	**)**	

MEMORANDUM AND ORDER

This matter is before the Court on a motion to compel discovery filed by Defendant Roland Hoeffener [ECF No. 27]. The Government charged Defendant with violating 18 U.S.C. § 2252A(a) by: (1) receiving over the internet videos and images of child pornography and (2) possessing two storage devices containing images and videos of child pornography. Defendant seeks to compel the Government to disclose the source code, software and manuals related to the software program investigators used to identify Defendant's computer.[1] The Government opposes Defendant's motion [ECF No. 36] on the grounds: (1) Defendant has not sufficiently demonstrated that the requested information is material to Defendant's defense and (2) the requested information is protected from disclosure as a sensitive law enforcement investigation technique. The parties attached exhibits to their motion and response. The Court conducted an

[1] The record reveals that, with regard to the software program used by law enforcement in this case, Defendant has received from the Government, at the hearing on Defendant's motion to compel: (1) a printout of a Powerpoint presentation about the installation and use of uTorrent version 2.2.1 (the file-sharing software on Defendant's computer at the time of the on-line investigation), (2) a compact disc depicting a simulation of how law enforcement personnel use the software program, and (3) the log of activity occurring during the on-line investigation of Defendant's computer, along with testimony further explaining those materials by a detective who helped create and trains law enforcement personnel on the use of the software program. See Hr'g Tr. [ECF No. 45]; Sealed Order [ECF No. 51] and Protective Order [ECF No. 52], filed June 23, 2017, as amended on July 10, 2017 [ECF No. 61]; list of exhibits from hearing on Def.'s mot. to compel [ECF No. 44]. Defendant also received from the Government: (1) the length of time the program has been used by the St. Louis Metropolitan Police Department and (2) a list of the program's authorized users. See Def's letter request for discovery dated Feb. 17, 2017 [ECF No. 27-2] and Gov't's letter response, dated Feb. 24, 2017 [ECF No. 27-3].

evidentiary hearing, and the parties filed post-hearing memoranda [ECF Nos. 53 and 55]. Defendant also attached several exhibits to his post-hearing brief. Having considered the parties' written materials and arguments, as well as the evidence adduced at the hearing, the Court denies Defendant's motion to compel discovery.

I. Background

A. The investigation

On December 15, 2012, Detective Bobby Baine of the St. Louis Metropolitan Police Department engaged in "an authorized Internet undercover operation."[2] Detective Baine used Torrential Downpour, a computer software program described (although not identified by name) in an April 29, 2013 affidavit that Detective Dustin Partney of the St. Louis County Police Department submitted in support of a search warrant. Detective Partney described Torrential Downpour as a "software program configured to search the BitTorrent network for [Internet Protocol ("IP")] addresses . . . offering to share or possessing files known to law enforcement that contain images/videos of child pornography."[3] During his on-line search, Detective Baine discovered an IP address later found to be associated with a Missouri computer.[4] According to Detective Partney's averments, Detective Baine "directly connected" with and downloaded several files from the computer.[5]

In his affidavit, Detective Partney identified two files Detective Baine downloaded during his December 2012 on-line investigation.[6] The two identified files used "spread.em.chan" at the

[2] Partney Aff. para. 4 [ECF No. 27-1].

[3] Partney Aff. para. 5.

[4] Partney Aff. para. 5.

[5] Partney Aff. para. 6.

[6] Partney Aff. para. 6.

beginning of each file name and contained images depicting minor females exposing their genitalia. One of the depicted females was characterized as "prepubescent."[7] Detective Partney viewed the files and "found them to contain" the described images.[8] Based on his training and experience, as well as Detective Baine's information, Detective Partney concluded that the computer "possess[ed] and distributed child pornography."[9]

Through information obtained from both the internet service provider for the IP address discovered by Detective Baine in December 2012 and a utility company, Detective Partney identified the computer as located at Defendant's residence in St. Louis County, Missouri.[10] Based on his training and experience, Detective Partney averred that "some people who collect child pornography tend to keep the images they obtain for extended periods of time and do not delete the images" or may "transfer the[] images to . . . digital media storage devices."[11]

Upon consideration of Detective Partney's affidavit and an application for a search warrant, a state court judge issued a warrant directing law enforcement officials to search Defendant's home for files and graphic images depicting pornography involving a person under the age of eighteen, as well as electronic data processing and storage devices, computers and computer systems, and other related items.[12] In the return and inventory for the search of Defendant's home, Detective Partney reported the seizure of multiple computers, hard drives, thumb-drives, Sim cards, CDs, digital cameras, and "tablet PC's" during execution of the search

[7] Partney Aff. para. 6.

[8] Partney Aff. para 8.

[9] Partney Aff. para 10.

[10] Partney Aff. paras. 7 and 9.

[11] Partney Aff. paras. 20 and 21.

[12] Search warrant, dated Apr. 29, 2013 [ECF No. 27-1].

warrant at Defendant's home on April 30, 2013.[13] As revealed by the two-page portion of the report available of record and statements of counsel, Detective Steve Grimm conducted a forensic examination of the seized items and filed a forensic report.[14]

B. The charges

In August 2016, the Government charged Defendant with three offenses. In Count I, the Government charged Defendant with violating 18 U.S.C. § 2252A(a)(2) by "knowingly recei[ving]" over the internet videos and images of child pornography between December 1, 2012 and April 30, 2013.[15] In Counts II and III, the Government charged Defendant with violating 18 U.S.C. § 2252A(a)(5)(B) by "knowingly possess[ing]" through April 30, 2013, two storage devices containing images and videos of child pornography (Counts II and III).[16] Each count includes a list identifying four or more visual depictions of a minor allegedly engaging in sexually explicit conduct.[17]

C. Defendant's motion to compel discovery

After Defendant requested and the Government refused to produce the manuals and

[13] Search warrant return and inventory, dated May 1, 2013 [ECF No. 27-1].

[14] See, e.g., Forensic report [ECF No. 36-6].

[15] Indictment, filed Aug. 25, 2016 [ECF Nos. 1, 2].

The Government recently filed a superseding indictment charging Defendant with the same alleged violations. Superseding Indictment, filed July 5, 2017 [ECF No. 56].

[16] Indictment, filed Aug. 25, 2016 [ECF Nos. 1, 2]; Superseding Indictment, filed July 5, 2017 [ECF No. 56].

[17] Indictment, filed Aug. 25, 2016; Superseding Indictment, filed July 5, 2017.

The only difference evident between the original and superseding indictments is that the superseding indictment omits from Count I two of the visual depictions of a minor allegedly engaging in sexually explicit conduct that were listed in Count I of the original indictment. The identification of the omitted visual depictions begins with "spread.em.chan." None of the visual depictions listed in each count of the superseding indictment begin with that phrase.

software for the program used by Detective Baine in his on-line investigation,[18] Defendant filed his motion to compel discovery seeking disclosure of "all discovery requested relating to the computer program . . . utilized by investigators in this matter[,] . . . includ[ing] user manuals, operation manuals, instruction manuals, documentation help or other technical manuals in possession of the investigators, and a copy of the program so that Defendant may conduct a forensic exam."[19] More specifically, Defendant requests a copy of the version of the software that Detective Baine used to "perform his search of Defendant's computer."[20]

Defendant argues the requested information is material to his defense and discoverable under Federal Rule of Criminal Procedure 16(a)(1)(E)(i), as well as the United States Supreme Court decisions in Brady v. Maryland, 373 U.S. 83 (1963) and Giglio v. United States, 405 U.S. 150 (1972) because the use of Torrential Downpour forms at least part of the basis of the receipt-of-child-pornography charge in Count I.[21] Without the technical data regarding Torrential Downpour, Defendant asserts his attorney cannot adequately analyze whether the software functioned correctly and whether the preliminary search and subsequent downloads of "potential evidence" violated the Fourth Amendment, comported with information in the search warrant, or constituted a form of computer hacking.[22] Furthermore Defendant contends the Government's use of Torrential Downpour to access his computer is "directly at issue" because the Government "will presumably" present evidence in its case-in-chief regarding the investigation.[23] Finally,

[18] See Def.'s letter request, dated Feb. 17, 2017 [ECF No. 27-2] and Gov't's response, dated Feb. 24, 2017 [ECF No.27-3].

[19] Def's mot. to compel at 1 [ECF No. 27].

[20] Def's mot. to compel at 3.

[21] Def.'s mot. to compel at 1, 3, 6-7.

[22] Def.'s mot. to compel at 1, 9.

[23] Def.'s mot. to compel at 3.

Defendant urges he needs the requested information to prepare for Detective Baine's cross-examination.[24] In support of his motion, Defendant cited United States v. Budziak, 697 F.3d 1105 (9th Cir. 2012) and provided a declaration of his expert, Michele Bush.

1. *Declaration of Michele Bush*[25]

Michele Bush, Defendant's computer forensics expert, stated she reviewed Detective Partney's affidavit in support of the search warrant, Detective Grimm's forensic report, the log "detailing the network activity between" Torrential Downpour and the IP address discovered during Detective Baine's on-line investigation, and the indictment.[26] Ms. Bush declared that the "log establishes that a connection was made between" Torrential Downpour software and Defendant's computer, but she needed to "validate the merits of the search warrant by identifying the information reported during the undercover investigation on the evidence seized from the suspect."[27] Ms. Bush stated she "had not had the opportunity to examine the digital media seized from [Defendant]'s residence" and relied on the forensic report.[28]

Ms. Bush described the BitTorrent network as allowing "users to download . . . parts of files from many different users which are then rebuilt into whole files."[29] She defined a "torrent" as "a text file proprietary to the BitTorrent network that contains instructions for torrent software, such as uTorrent . . . , on how to download a file or sets of files on the BitTorrent

[24] Def.'s mot. to compel at 7-9.

[25] ECF No. 27-4.

[26] Bush Decl. paras. 4, 5, and 6 [ECF No. 27-4].

[27] Bush Decl. para. 11.

[28] Bush Decl. para. 11. The Government attorney stated that the Government offered Defendant "full access to the forensic images of the Defendant's computer items from which an expert should be able to detect any government intrusion." Gov't response to Def's mot. to compel at 26.

[29] Bush Decl. para. 8.

network." [30] As she explained, "[t]orrent files do not contain user data, such as images or videos," but rather an index of information about the files associated with the torrent.[31] Ms. Bush described "infohash" as a "unique[] identifie[r of a] 'torrent' on the BitTorrent network."[32] She noted the log identified Defendant's BitTorrent "software application utilized to connect to the BitTorrent network as uTorrent version 2.2.1."[33]

Additionally, Ms. Bush explained her understanding of Torrential Downpour as "a modified version of publicly available file sharing software used exclusively by law enforcement"[34] that differed from publicly available file sharing software "in at least three ways: 1) it downloads files from a single IP address, 2), it does not share files, and 3) it creates a detailed log of network activity between the software and the suspect['s computer]."[35] Finally, Ms. Bush opined:

> there is no credible evidence that the files identified as suspect child pornography in Detective Partney's Affidavit for Search Warrant and included as part of Count One of the Indictment were publicly available on [Defendant's] computer identified at the IP address[discovered during Detective Baine's on-line investigation]. In addition, it remains my opinion that law enforcement's proprietary software [Torrential Downpour] needs to be tested by a qualified third-party to determine its functionality and accuracy.[36]

(Footnote added.)

[30] Bush Decl. para. 9. When not referring specifically to the uTorrent software, the Court refers to the type of software program Ms. Bush refers to as "torrent software" as "BitTorrent software."

[31] Bush Decl. para. 9.

[32] Bush Decl. para. 10.

[33] Bush Decl. para. 11.

[34] Bush Decl. para. 6.

[35] Bush Decl. para. 6.

[36] Bush Decl. para. 17.

In her declaration, Ms. Bush set forth several concerns about Torrential Downpour and the content of the forensic report.[37] Ms. Bush noted "[i]t is unknown how the BitTorrent [network] protocol affects Torrential Downpour's ability to successfully operate on the network and identify suspects" because, unlike other BitTorrent software, Torrential Downpour does not "share data" with other computers on the network.[38] Ms. Bush explained that the BitTorrent network protocol "can eventually restrict [a non-sharing computer] from receiving data, per a 'tit-for-tat' policy requiring users to contribute data in order to obtain data."[39]

In addition, Ms. Bush stated "[i]t is unknown if Torrential Downpour can identify a [computer] containing only the torrent of suspect[ed] child pornography without possessing its content."[40] This concern arose out of her view that a torrent does not consist of user data, i.e., images or videos a user can see but rather information about the torrent, which is used by the BitTorrent software to download information for a user's use.[41]

Ms. Bush also questioned certain aspects of the forensic report in her effort to "validate the merits of the search warrant by identifying the information reported during the undercover investigation on the evidence seized from the suspect."[42] In particular, Ms. Bush declared the forensic report "revealed an examination was conducted on approximately eight hard drives installed with operating systems [and o]nly two hard drives were found to contain file sharing

[37] The complete forensic report is not available of record.

[38] Bush Decl. para. 8.

[39] Bush Decl. para. 8.

[40] Bush Decl. para. 9.

[41] Bush Decl. paras. 9 and 10.

[42] Bush Decl. para. 11.

software including Lime Wire and eMule."[43] The report, Ms. Bush noted, was "silent with regard to locating [on any of the seized items] the uTorrent software version 2.2.1, the torrent identified [during the on-line investigation], or the files of suspected child pornography specifically downloaded" during the on-line investigation, i.e., those starting with "spread.em.chan."[44]

Additionally, Ms. Bush observed, the forensic report disclosed "the majority of the suspect child pornography was located within system locations on the hard drive, compressed backup files, external devices, and possibly encrypted containers, so it is unknown if any of those locations would have been publicly available."[45] Based on her

> experience . . . conduct[ing] forensic exams on computers seized during undercover investigations and f[inding] evidence contrary to the information reported by law enforcement's software such as file sharing [being] turned off prior to the undercover investigation or that files only existed in private folders that were not available for sharing and should not have been identified by law enforcement's automated software,

Ms. Bush questioned whether Torrential Downpour may have accessed non-public information on Defendant's computer.[46]

Ms. Bush also stated that her "forensic training" taught her she "cannot rely on" a software program that has not been tested or validated by her or available for testing by "industry peers."[47] Ms. Bush opined that Torrential Downpour "needs to be tested by a qualified third-

[43] Bush Decl. para. 12.

[44] Bush Decl. para. 12; see also para. 13.

[45] Bush Decl. para. 12. Ms. Bush observed that "[o]ther than the existence of child pornography, no connection was made between the undercover investigation and evidence seized from [Defendant]'s residence that would indicate he was the suspect identified." Id.

[46] Bush Decl. para. 13.

[47] Bush Decl. para. 14.

party to determine its functionality and accuracy."[48]

D. Government's response to motion

The Government opposes Defendant's motion on the grounds the requested information "is law enforcement sensitive and not material to [Defendant's] defense."[49] More specifically, the Government contends the requested information is protected by a law enforcement privilege that prohibits disclosure of a "sensitive law enforcement technique."[50] With respect to materiality, the Government urges Defendant has not demonstrated a sufficient basis to support disclosure of the user manuals, source code or software for the program used by the investigator.[51] In support of its position, the Government cited, in relevant part, United States v. Pirosko, 787 F.3d 358 (6th Cir. 2015), and provided an affidavit of its computer forensics expert, Deteective Robert Erdely.

1. *Affidavit of Detective Robert Erdely*[52]

Detective Robert Erdely averred that he helped create and conducts training of law enforcement personnel for the Torrential Downpour software program used by "law enforcement organizations . . . to identify potential possessors and distributors of child pornography over the BitTorrent peer-to-peer (P2P) sharing network."[53] Detective Erdely described Torrential Downpour as different from other available BitTorrent software in that law enforcement investigators do not need to look to outside websites to obtain .torrent files and infohashes

[48] Bush Decl. para. 17.

[49] Gov't's response Def.'s mot. to compel at 1 [ECF No. 36].

[50] Gov't's response Def.'s mot. to compel at 22-26.

[51] Gov't's response Def.'s mot. to compel at 10-22.

[52] ECF No. 36-2.

[53] Erdely Aff. para. 3.

because law enforcement maintains such information for use during investigations.[54] Additionally, Torrential Downpour downloads information from a "single source" or from a "solitary download candidate," rather than from "many sharing computers," which the BitTorrent network is designed to do because "it speeds up the download times."[55] Torrential Downpour, unlike other BitTorrent software, "does not share any of the content downloaded during an investigation."[56]

Detective Erdely explained that a non-law enforcement user of the BitTorrent network must obtain a torrent file from an outside website and use it to "receive or distribute" information over the BitTorrent network.[57] To access information available through the network, a user loads the torrent (a file designated by ".torrent")[58] into the computer's BitTorrent software on the user's computer and the BitTorrent software initiates contact with the BitTorrent network to locate "download candidates."[59] A download candidate is a computer on the BitTorrent network "looking for or . . . actively sharing the same file(s) described by the .torrent file."[60] The computer connecting with the BitTorrent network provides the network with certain information, including the "computer's IP address and the unique identifier of the .torrent" sought or available

[54] Erdely Aff. para. 11.

[55] Erdely Aff. para. 12.

[56] Erdely Aff. para. 13.

[57] Erdely Aff. para. 6.

[58] As Ms. Bush had declared, Detective Erdely averred that "[a] torrent file does not contain the actual file itself (in this case the actual child pornography image), [but] only contains information about the file(s)." Erdely Aff. para. 6.

[59] Erdely Aff. paras. 8-10.

[60] Erdely Aff. para. 8.

to share.[61] "Both the sharing computer and the downloading computer must have the same torrent file (identified through a unique identifier called an 'infohash')" to download information available through the BitTorrent network.[62]

Once a match is located, the BitTorrent software "can then connect to 1 or many download candidates and request to download the pieces of the files needed."[63] The BitTorrent network shares files "by downloading 'pieces,'" which, as Detective Erdely explained, "are not typically the whole file but instead a piece of one file or several files."[64] The BitTorrent software finds the download of a piece "successful" by comparing its SHA-1 hash value to the value in the torrent file and concluding those values match or are the same.[65] "[B]y default, [the BitTorrent software, other than Torrential Downpour,] shares downloaded data back to other BitTorrent [network] users from whatever location the data was saved to, which would include an external hard drive."[66]

[61] Erdely Aff. paras. 9 and 10.

[62] Erdely Aff. para. 8. More specifically, Detective Erdely characterized as "impossible" the downloading of information through the BitTorrent network unless the sharing and downloading computers "hav[e] the same .torrent file." Id.

Detective Erdely also averred that an infohash is "a very reliable way to uniquely identify" information "being shared on the BitTorrent file sharing network" because it is based on the Secure Hash Algorithm ("SHA-1") developed by the National Institute of Standards and Technology and the National Security Agency. Erdely Aff. paras. 7, 9. In support of his opinion about the reliability of the infohash, Detective Erdely stated the "odds" of a SHA-1 failing, i.e., two different files "producing the same SHA-1 hash," is "1 in 1,461,501,637,330,900,000,000,000,000,000,000,000,000,000,000,000." Erdely Aff. para. 7.

[63] Erdely Aff. paras. 8 and 16.

[64] Erdely Aff. para 16.

[65] Erdely Aff. para 16.

[66] Erdely Aff. para. 22. More specifically, Detective Erdely explained:

> [t]he data will continue to be shared as long as the [BitTorrent] program is running, the computer is connected to the internet, and the .torrent and data remain in the location where they had been downloaded to and the BitTorrent user had not taken an affirmative step to stop sharing that particular .torrent.

Detective Erdely averred that uTorrent software does not have a "'default download' folder" but, instead, a user may save downloaded torrent files to a folder the user configured or "another location, even external hard drives, encrypted drives or network attached storage devices."[67] Additionally, based on his "hundreds of investigations," Detective Erdely stated "it is common for users downloading child pornography to copy and/or move files from location to location, often deleting the file from the original location."[68] In response to Ms. Bush's concern that the forensic report failed to mention that uTorrent was discovered on any of the items seized[69] from Defendant's home, Detective Erdely pointed to a reference in the portion of the forensic report available of record stating that uTorrent was installed on a seized item.[70]

Torrential Downpour, Detective Erdely averred, "never obtains any unshared information from any computer running" BitTorrent software.[71] Rather, the law enforcement software "'searches' for download candidates in [the] same that any public user of the" BitTorrent network searches and "only searches for information that a user has already made public by the very use of the uTorrent" software.[72] As Detective Erdely described, "[e]ach and every location where a user downloads file(s) . . . becomes 'publicly shared.'"[73] Detective Erdely explained

Id.

[67] Erdely Aff. para. 15.

[68] Erdely Aff. para. 15.

[69] The exact nature of the items seized from Defendant's home is not now available of record. Through the return after the search, the Court understands law enforcement's execution of the search warrant resulted in the seizure of multiple computers, harddrives, thumbdrives, Sim cards, cds, digital cameras, and "tablet pcs." See Return and Inventory at ECF No. 36-1.

[70] Erdely Aff. para. 15; see Forensic Report [ECF 36-6].

[71] Erdely Aff. para. 19.

[72] Erdely Aff. paras. 19-21.

[73] Erdely Aff. para. 15.

that, due to the BitTorrent software's matching of SHA-1 hash values of downloaded pieces, "it would be '**absolutely impossible**' to randomly download files from a suspect's computer which are from 'unshared folders'" (emphasis in original).[74]

Detective Erdely further asserted that, "at the FBI's direction," an independent company performed validation testing of Torrential Downpour.[75] Specifically, the company tested Torrential Downpour's software and its source code to verify: (1) that it "contacts and downloads from the [IP] address and port specified," (2) that it "properly conducts . . . a 'single source download' or . . . will only ever download from the one IP address specified," (3) that it is "incapable of sharing the downloaded content out to other [B]it[T]orrent [network] users," and (4) that it "accurately places the downloaded content into the evidence folder created for each and every investigation."[76] The testing company concluded Torrential Downpour "passed all operational/validation tests."[77] Detective Erdely also noted that the company found Torrential Downpour contained "a minor bug:" "if a file path became too long, the program would stop performing investigations."[78] The discovered program bug, Detective Erdely averred, was fixed.[79]

With regard to the importance of protecting Torrential Downpour's software and source code from discovery, Detective Erdely averred:

> If the source code or certain other details about [Torrential Downpour] became public, child pornography distributors could find a way to avoid detection from

[74] Erdely Aff. para. 16.

[75] Erdely Aff. paras. 17-18.

[76] Erdely Aff. para 17.

[77] Erdely Aff. para. 18.

[78] Erdely Aff. para. 18.

[79] Erdely Aff. para. 18.

> [Torrential Downpour] and could render that tool of law enforcement ineffective. Additionally, the .torrent[s] and the hash values of the files being investigated could hinder future investigations once th[e] identifier to the illegal files became public. The infohash becoming public would also allow others to quickly find and download these child pornography files.[80]

(Footnote added.)

E. The hearing

At the evidentiary hearing, Defendant, through counsel, stated that the written motion and Ms. Bush's attached declaration demonstrated the requested information was material, and he would not present additional evidence during the hearing.[81] The Government introduced four exhibits[82] and the testimony of Detective Erdely.[83] During his testimony, Detective Erdely described in more detail: (1) the manner in which the BitTorrent network, uTorrent software, and Torrential Downpour software work; (2) the results of the validation testing of the Torrential Downpour software; and (3) the sensitive and confidential nature of the Torrential Downpour software, source code, and manuals.

Detective Erdely testified that peer-to-peer file sharing networks, such as the BitTorrent network, "look to multiple computers [to download material] for redundancy (in case one of the sharing computers goes offline during a download) and speed (usually a computer has greater download than upload speed)."[84] When the pieces making up the files in a torrent are

[80] Erdely Aff. para. 14.

[81] Hr'g Tr. at 8 [ECF No. 45].

[82] Exhibit 1 is Detective Erdely's curriculum vitae. Hr'g Tr. at 10. Exhibit 2 is a printout of a PowerPoint presentation Detective Erdely created to show how uTorrent version 2.2.1 is downloaded to a computer and downloads a torrent to a user's computer. Hr'g Tr. at 18. Exhibit 3 is a compact disc made by Detective Erdely simulating a law enforcement session using Torrential Downpour version 1.0 and uTorrent version 2.2.1. Hr'g Tr. at 39. Exhibit 4 is the log from Detective Baine's December 2012 on-line investigation. Hr'g Tr. at 69.

[83] Hr'g Tr. at 9-162.

[84] Hr'g Tr. at 20-21.

downloaded from the BitTorrent network, the BitTorrent software puts the pieces in the correct order to provide data for the user to view.[85]

During installation of the uTorrent software on the user's computer, uTorrent notifies and requires consent of the user that downloaded files are made available to others.[86] Additionally, the user must allow the uTorrent software to be an exception to any firewall on the user's computer.[87] Once installed, the user must allow the uTorrent software to start each time the computer's operating system starts.[88] Each time the uTorrent software starts, it offers to computers seeking information through the BitTorrent network the files on the user's computer that are available for sharing, even if the user's computer is not actively downloading material from the BitTorrent network.[89] The user may use a "stop button" in the uTorrent program to stop sharing information with the BitTorrent network during a session, but may not set uTorrent software to prevent it from uploading information available for sharing.[90]

The first version of Torrential Downpour was available in October 2012.[91] Detective Erdely explained that, through use of Torrential Downpour, an investigator sees the IP addresses of those computers seeking to obtain the torrent the investigator is investigating.[92] The

[85] Hr'g Tr. at 18.

[86] Hr'g Tr. at 21-22.

[87] Hr'g Tr. at 23. If a user does not allow uTorrent to make an exception to the firewall, then other computers are unable to initiate connections with the firewalled computer. Id. at 146. A firewall stops inbound communication but not outbound information. Id. at 146-47. So a uTorrent user accessing the BitTorrent network could see a firewalled computer as a download candidate but could not connect to and download from that computer. Id. at 147-48. Torrential Downpour cannot connect to a firewalled computer. Id. at 149.

[88] Hr'g Tr. at 23.

[89] Hr'g Tr. at 23, 29.

[90] Hr'g Tr.. at 31, 94-99.

[91] Hr'g Tr. at 63.

[92] Hr'g Tr. at 43, 58.

investigator then chooses a computer's IP address and port for Torrential Downpour to connect to, then Torrential Downpour ascertains whether the computer has the investigated torrent, and, if so, directly connects to the computer.[93]

Torrential Downpour provides a record or log of the date, time, and infohash of the investigation, the activity occurring during the investigation, the path and file name investigated, and the investigated computer's IP address, port identifier, and BitTorrent software[94] As Detective Erdely described, the log for Detective Baine's December 2012 on-line investigation reports that the investigated computer had all pieces of the torrent investigated, "did not need anything from the investigating computer," and provided the data during one connection.[95] After a download, law enforcement personnel assess whether the downloaded files meet the requirements for "child pornography" as defined by the charging jurisdiction.[96]

Torrential Downpour participates in the BitTorrent network without sharing information it obtains through the network because the BitTorrent network protocol allows that participation.[97] More specifically, the BitTorrent network has a "choked" state preventing a computer from obtaining information available through the network when the computer is not sharing information, and an "optimistically unchok[ed]" state when the network unchokes the

[93] Hr'g Tr. at 43-44. If the computer does not have the investigated infohash, communication with the computer stops. Id. at 48.

[94] Hr'g Tr. at 45-47, 69.

[95] Hr'g Tr. at 71-72, 128.

[96] Hr'g Tr. at 140.

Detective Erdely stated he was aware of circumstances when investigators subsequently find no child pornography on computers, not due to error by the law enforcement investigation, but because the pornography was deleted, the computer involved in the investigated download was not present, or someone other than the computer user, such as a neighbor, was using the investigated user's connection to the internet. Hr'g Tr. at 130.

[97] Hr'g Tr. at 51, 127-28.

computer to give it data.[98] Detective Erdely noted that without this feature the network would not work because the first time a computer accesses the network it has no data to share.[99]

The BitTorrent network also supports single source downloads.[100] A non-law enforcement user of the BitTorrent network may obtain such downloads by using an IP filter to filter activity into the user's computer so that only one IP address can communicate with the user's computer.[101] Torrential Downpour ensures single source downloads.[102]

Torrential Downpour does not access encrypted material on a computer, but while uTorrent is "downloading to an encrypted volume" the data "is in a decrypted state" and shared.[103] When the user "unmounts [the downloaded data] so it is no longer accessible," the sharing stops because the data is now encrypted and BitTorrent software "cannot see" the encrypted data.[104] Encrypted data "cannot be accessed unless it is decrypted and connected to [or] in" a computer.[105] Additionally, if a user accesses data through a Virtual Private Network, Torrential Downpour "still sees" the computer's IP address, but at a different location, and law enforcement is able to locate the computer after further investigation of the log information.[106]

With regard to the validation testing of Torrential Downpour, the testing company found "no errors in . . . single source downloads, how logs are written, how [the] infohash is

[98] Hr'g Tr. at 51.

[99] Hr'g Tr. at 51.

[100] Hr'g Tr. at 83-84.

[101] Hr'g Tr. at 83-84.

[102] Hr'g Tr. at 86.

[103] Hr'g Tr. at 142.

[104] Hr'g Tr. at 142.

[105] Hr'g Tr. at 142-43.

[106] Hr'g Tr. at 144.

documented, [or the] dates and times" recorded.[107] An error would exist, Detective Erdely stated, if Torrential Downpour allowed reaching out to a different IP address than the investigated IP address, and no such error was found during the validation testing.[108]

According to Detective Erdely, Torrential Downpour cannot go into unshared portions of an investigated computer and cannot override settings on that computer.[109] Additionally, Detective Erdely has not found a report that Torrential Downpour has accessed unshared parts of a computer or overridden a computer's settings.[110]

With respect to the need to protect the Torrential Downpour program from public disclosure, Detective Erdely explained that:

> [t]he torrents we investigate would be exposed, the hashes of the files we investigate that we found that relate to child exploitation [would be available if the program is disclosed]. The version of software, we appear like as we're conducting these investigations [would be available if the program is disclosed]. People could change one little bit of the torrent, not really changing the downloads but now it's a different infohash [if they had the requested information about Torrential Downpour, then] we have to start from scratch. [Additionally, those having the requested information] could develop ways to avoid trading with our software based on characteristics of the software. And certainly we don't want to get the hash values [of the child pornography] that we investigate out to the general public.[111]

(Footnote added.) Detective Erdely described as "extremely confidential and law enforcement sensitive" "[t]he source code and the program and the infohashes we investigate, the hashes of

[107] Hr'g Tr. at 131-36.

Detective Erdely also testified that all Torrential Downpour versions since version 1.0 used in this case have been created to provide enhancements, and not to resolve "bugs" beyond the "bug" discovered during the validation testing. Id. at 153.

[108] Hr'g Tr. at 134.

[109] Hr'g Tr. at 72.

[110] Hr'g Tr. at 74.

[111] Hr'g Tr. at 62-63, 156.

the files we investigate, [and] the version of software we appear as on the network."[112] If that information is shared with the public, Detective Erdely testified, "you've just taken the ability of law enforcement away to conduct these investigations, leaving pedophiles and child predators out there to do what they want."[113] In summary, Detective Erdely described the sensitive nature of the Torrential Downpour software as follows:

> It's designed to download child pornography. It interacts with a law enforcement system that I'm the administrator of. The software will download infohashes relating to child exploitation. It would reveal the hash values of the files we're investigating. It would identify to the people that have it how we appear on the network. Any of these actions or any of these things I described could be altered to subvert our efforts and avoid detection, whether that be change the torrents, change the hashes of the files, [or] not allow communication with our software.[114]

(Footnote added.)

Furthermore, as Detective Erdely explained, law enforcement personnel must be licensed to use Torrential Downpour, and the program's source code is "compiled" to prevent changes to it.[115] Law enforcement personnel using the program receive "the executable" file of the software for free "for the purpose of conducting investigations, not to redistribute" it.[116] Moreover, the licensed law enforcement personnel using Torrential Downpour do not have access to and are not given the program's source code.[117]

[112] Hr'g Tr. at 115.

[113] Hr'g Tr. at 115.

[114] Hr'g Tr. at 156-57.

[115] Hr'g Tr. at 63-64.

[116] Hr'g Tr. at 63-64, 92-93, 111-14.

[117] Hr'g Tr. at 63-64, 92-93, 111-14.

With regard to the user manual for Torrential Downpour, Detective Erdely stated it contains information that requires protection.[118] In particular, Detective Erdely explained the manual contains information about the law enforcement server, its location, and how law enforcement accesses it.[119]

F. Post-hearing briefs

Defendant filed a post-hearing brief with several attachments. None of the attachments contained additional declarations or other evidentiary material from Defendant's expert or any other individual responding to the testimony and exhibits presented during the hearing. In his post-hearing brief, Defendant asked the Court either: (1) to order the Government to provide validation testing information related to Torrential Downpour or (2) to strike and deem inadmissible at trial Detective Erdely's affidavit and testimony regarding that testing.[120] Additionally, Defendant requested the Court consider his motion to compel as a motion for a subpoena under Federal Rule of Criminal Procedure 17(c), if the Court denies the motion to compel.[121]

The Government filed a response to Defendant's post-hearing brief.[122] The Government opposed Defendant's request that the Court consider the motion to compel as a request for a subpoena under Rule 17 on two grounds. First, the Government argued the requirements supporting disclosure of information under Rule 17(c) are different than the requirements for

[118] Hr'g Tr. at 75.

[119] Hr'g Tr. at 75.

[120] Def.'s post-evidentiary hr'g mem. sup. Def.'s mot. to compel at 16 [ECF No. 53]. See also Def.'s letter to Gov't, dated June 13, 2017 [ECF No. 46]; Gov't letter response, dated June 23, 2017 [ECF No. 53-4].

[121] See "Wherefore" para. at page 21 of Def.'s post-evidentiary hr'g mem. sup. Def.'s mot. to compel [ECF No. 55].

[122] See Gov't's response to Def.'s post hearing mem. at 9-11.

disclosure of information under Rule 16(a)(1)(E)(i) and Defendant did not address the requirements of Rule 17(c).[123] Second, the Government contended that Rule 17(c) was not intended to serve as a discovery tool.[124]

II. Standard

District courts have broad discretion to resolve motions to compel discovery in criminal cases. United States v. Hintzman, 806 F.2d 840, 846 (8th Cir. 1986). A district court's decision regarding a motion to compel discovery is proper if, considering the circumstances, the decision is not "a gross abuse of discretion resulting in fundamental unfairness at trial." Id. (internal quotation marks omitted) (quoting Voegeli v. Lewis, 568 F.2d 89, 96 (8th Cir. 1977)).

III. Discussion

Defendant argues the requested information is material to his defense and, therefore, discoverable under Federal Rule of Criminal Procedure 16(a)(1)(E)(i)[125] based on four

[123] See Gov't's response to Def.'s post hearing mem. at 9-11.

[124] See Gov't's response to Def.'s post hearing mem. at 9-11.

[125] Defendant also cites the United States Supreme Court decisions in Brady v. Maryland, 373 U.S. 83 (1963) and Giglio v. United States, 405 U.S. 150 (1972), in support of his motion to compel discovery. The Government did not expressly respond to this basis for disclosure.

In Brady, the United States Supreme Court found that due process requires the Government to provide a defendant any evidence in the Government's possession which is favorable to the defendant and material to the guilt or punishment of the defendant. Brady, 373 U.S. at 87. The Government's obligation under Brady also requires the Government to provide a defendant evidence related to the credibility of a government witness when the reliability of the witness may be determinative of the defendant's guilt or innocence. Giglio, 405 U.S. at 153-54. Importantly, disclosure under Brady is not a rule of discovery but "a rule of fairness and minimum prosecutorial obligation." United States v. Miller, 698 F.3d 699, 704 (8th Cir. 2012) (internal quotation marks and citation omitted).

"The Government has no duty [under Brady] to disclose evidence that is neutral, speculative, or inculpatory, or evidence that is available to the defense from other sources." United States v. Pendleton, 832 F.3d 934, 940 (8th Cir. 2016). To support disclosure under Brady, a defendant must make a "preliminary showing" that the requested information is exculpatory. United States v. Roach, 28 F.3d 729, 734 (8th Cir. 1994).

To the extent Defendant may seek disclosure of the requested information under Brady and Giglio, Defendant has neither argued nor demonstrated either the exculpatory nature of any of the requested information or how the requested information could be used for impeachment. See United States v. Huber, 404 F.3d 1047, 1062 (8th Cir. 2005) (concluding Brady was not violated by a late disclosure of a document that did not contain grounds.[126] First, Defendant asserts the use of Torrential Downpour forms at least part of the basis for the receipt-of-child-pornography charge in Count I and Defendant needs the requested Torrential Downpour information to assess whether Count I is “accurate, legitimate and proper.”[127] Second, Defendant contends the use of Torrential Downpour to access Defendant’s computer is “directly at issue,” because the Government will “presumably present” in its case-in-chief evidence of the investigation.[128] Third, Defendant argues the requested information is needed to prepare for the cross-examination of Detective Baine.[129] Finally, Defendant urges the use of Torrential Downpour is the sole basis of the search warrant and, without the requested information, his attorney cannot adequately analyze whether the software was functioning correctly or whether the preliminary on-line search and subsequent downloads of “potential evidence” violated the Fourth Amendment, comported with information in the search warrant, or constituted a form of computer hacking.[130] In support of his position that the requested information is material, Defendant relies on his expert’s declaration and the Ninth Circuit’s decision in Budziak, supra.

The Government opposes the motion on the ground Defendant has not demonstrated the requested information is material to a defense for purposes of Rule 16. In particular, the Government argues the defense expert provides only a general description of the information

exculpatory evidence and did not contain information that could be used for impeachment). Therefore, the Court denies without prejudice Defendant’s motion to compel under Brady and Giglio.

[126] For ease of reference, the Court addresses Defendant’s arguments in a sequence that may not reflect the order in which Defendant presented his arguments.

[127] Def.’s mot. to compel at 1, 3, 6-7.

[128] Def.’s mot. to compel at 3.

[129] Def.’s mot. to compel at 7-9.

[130] Def.’s mot. to compel at 1, 3, 9.

sought and conclusory allegations of materiality.[131] The Government relies on the Sixth Circuit's decision in Pirosko, supra, as support for its position that Defendant has not demonstrated Rule 16 materiality. Additionally, the Government contends the requested information constitutes a sensitive law enforcement investigative technique protected from disclosure by a law enforcement privilege.

A. Materiality

1. *Standard*

Federal Rule of Criminal Procedure 16(a)(1)(E)(i) requires the Government to permit a defendant, upon the defendant's request, "to inspect and to copy or photograph . . . books, papers, documents, [and] data, [among other items] . . . or copies or portions of any of these items" that are in the Government's possession, custody, or control and are "material to preparing the defense." A defendant may examine specified information in the Government's possession that is "material to the preparation of [the defendant's] defense against the Government's case-in-chief" or the defendant's defense on the merits. United States v. Armstrong, 517 U.S. 456, 463 (1996) (concluding that Rule 16(a)(1)(C), a predecessor to Rule 16(a)(1)(E), does not apply to a defendant's request to examine Government information for a selective prosecution claim, because that claim is not a defense on the merits).

The Eighth Circuit defines "material" information for purposes of Rule 16 as information that is "helpful to the defense." United States v. Vue, 13 F.3d 1206, 1208 (8th Cir. 1994) (discussing Rule 16(a)(1)(C), the predecessor to Rule 16(a)(1)(E)(i)).[132] However, importantly, a showing of materiality requires more than "a mere conclusory allegation" of the requested

[131] Govt's response Def.'s mot. to compel at 13.

[132] Rule 16(a)(1)(C), a predecessor to Rule 16(a)(1)(E)(i), provided in relevant part for a defendant's inspection, copying, and photographing of books, documents, and other specified items within the Government's possession, custody or control if the defendant requested discovery of those items and the items were "material to the preparation of the defendant's defense."

information's materiality. United States v. Krauth, 769 F.2d 473, 476 (8th Cir. 1985) (discussing predecessor Rule 16(a)(1)(C)).

To demonstrate materiality, a defendant must show "more than that [the requested information] bears some logical relationship to the issues in the case." United States v. Ross, 511 F.2d 757, 762 (5th Cir. 1975) (discussing predecessor Rule 16(b));[133] accord United States v. Jordan, 316 F.3d 1215, 1250 (11th Cir. 2003) (discussing predecessor Rule 16(a)(1)(C)). In particular, a defendant must show the pretrial disclosure of the requested information would "enable the defendant significantly to alter the quantum of proof in his favor." Ross, 511 F.2d at 763; accord Jordan, 316 F.3d at 1250. More specifically, a defendant must show "case-specific facts which would demonstrate the materiality of the information sought." United States v. Santiago, 46 F.3d 885, 895 (9th Cir. 1995) (discussing predecessor Rule 16(a)(1)(C)); accord Krauth (finding a discovery motion properly denied where the defendant failed to produce evidence that the requested information would be helpful to the defense).

With regard to child pornography cases addressing requests for the disclosure of information related to law enforcement software programs under the materiality requirement of Rule 16, the success of a defendant's motion to compel depends on the specificity of the defendant's evidentiary support for the motion in demonstrating the need for the requested information to defend the charges. In Budziak, the United States Court of Appeals for the Ninth Circuit concluded that the defendant made a sufficient showing "that discovery of the EP2P software[, an enhanced version of LimeWire file-sharing software used by investigators,] was material to preparing his defense." Budziak, 697 F.3d at 1112-13. In particular, the defendant,

[133] Rule 16(b), a predecessor to Rule 16(a)(1)(E)(i), provided in relevant part for a defendant's inspection, copying and photographing of books and other specified items in the Government's possession, custody, or control when the defendant requested discovery of those items and showed the "materiality [of the requested items] to the preparation of the defendant's defense."

who was charged in relevant part with distribution of child pornography due to two investigators' downloads of child pornography from the defendant's computer, sought disclosure of "the EP2P program and its technical specifications." Id. at 1107, 1109, 1112. The defendant had, the Ninth Circuit found, "identified specific defenses to his distribution charge that discovery on the EP2P program could potentially help him develop." Id. at 1112. In particular, the Ninth Circuit stated the defendant

> presented evidence suggesting that [(1)] the FBI may have only downloaded fragments of child pornography files from [the defendant's] "incomplete" folder, making it "more likely" that he did not knowingly distribute any complete child pornography files [to the investigators] and [(2)] the [investigators] could have used the EP2P software to override his sharing settings.

Id. Importantly, the Ninth Circuit found it was "logical to conclude that the functions of the program were relevant to his defense" because "the distribution charge against [the defendant] was premised on the FBI's use of the EP2P program to download files from him." Id. The Ninth Circuit held the district court abused its discretion in denying the defendant "discovery on the EP2P program." Id. at 1113.

In Pirosko, the United States Court of Appeals for the Sixth Circuit concluded the defendant's requested disclosure of "the law enforcement tools and records used . . . to search [the defendant]'s computer equipment" did not satisfy Rule 16's materiality requirement. Pirosko, 787 F.3d at 368. The Sixth Circuit found the "purpose of [the defendant]'s motion to compel [was] not to aid in the preparation of his defense, but to contradict the district court's finding of distribution [of child pornography] at sentencing." Id. When addressing the Government's argument that a law enforcement privilege protected the requested information from disclosure, the Court distinguished Budziak on the ground the defendant in that case provided evidence of government error. Id. at 366. The defendant's evidentiary support for his motion to compel was a letter with one sentence summarily questioning the government's affidavit as not showing "which tools, which records, or the means by which those records were created" and "leaving otherwise answerable questions unanswered." Id. The Sixth Circuit concluded the "lone allegation [in the letter was] simply not enough to overcome the numerous facts supporting the government's position that it legitimately obtained child pornography from [the defendant]'s shared folders." Id.

The United States Court of Appeals for the First Circuit also provides useful guidance in United States v. Chiaradio, 684 F.3d 265, 271-72, 276-78 (1st Cir. 2012). There the First Circuit affirmed the denial of a defendant's motion to compel production of the source code for law enforcement software used by investigators to identify the defendant's computer as sharing child pornography through the file-sharing software on the defendant's computer. The defendant argued he needed the source code to determine whether he "could credibly challenge the reliability of the technology and . . . block the [Government's] expert testimony . . . about the [law enforcement software] program and how it implicated the defendant." Id. at 277. The First Circuit did not resolve the issue of the source code's materiality under Rule 16, because it found the defendant was not prejudiced due to other information the defendant had received relating to the on-line investigation. Id. at 277-78.

2. *Showing of materiality*

(a) Materiality based on Count I

Defendant asserts the use of Torrential Downpour forms at least part of the basis of the receipt-of-child-pornography charge in Count I of the indictment and Defendant needs the requested information to assess whether Count I is "accurate, legitimate and proper."[134]

[134] Def.'s mot. to compel at 3, 7.

Defendant urges that "[w]ithout access to the technical data behind Torrential Downpour the defense would be relying on blind faith regarding the programming of the software, the methodology respecting its use, it[s] error rate, whether it is subject to peer review, and every other aspect."[135] Defendant contends that the absence of downloaded images on the seized items, as mentioned in Ms. Bush's declaration, supports reasonable doubt with regard to the charge in Count I. The Government urges there are plausible explanations for the absence of downloaded files on the seized items. Specifically, the Government states Defendant could have moved the downloaded files into inaccessible encrypted areas or deleted the downloaded files.

While the absence of downloaded images and videos on the seized items may arguably help to demonstrate reasonable doubt with regard to Count I of the original indictment, the absence of the downloaded images and videos on seized items does not assist with the development of reasonable doubt regarding Count I of the superseding indictment. Count I of the original indictment explicitly mentioned as material constituting child pornography two files that the log of Detective Baine's December 2012 on-line investigation reported as downloaded during that investigation. The downloaded files are identified in the log and in Count I of the original indictment as beginning with the phrase "spread.em.chan." Count I of the superseding indictment also specifically identifies certain images and videos of child pornography, but none of the references begin with the phrase "spread.em.chan." Therefore, nothing in the pending receipt-of-child-pornography charge reveals that the charge is based, to any extent, on materials downloaded from Defendant's computer while Detective Baine used Torrential Downpour in December 2012. Additionally, no other material in the available record supports a conclusion that any file downloaded by Detective Baine during his December 2012 on-line investigation

[135] Def.'s mot. to compel at 6.

forms any basis for the receipt-of-child-pornography charge in Count I of the superseding indictment.

To the extent Defendant relies on Budziak as support for this ground, that decision is distinguishable. In Budziak, the defendant there was charged with distribution of child pornography based only on the investigators' download of alleged child pornography material during their on-line investigations. Here, Defendant is not charged with distribution of child pornography and, as noted above, the charges pending against Defendant are not based on downloaded material obtained during Detective Baine's December 2012 on-line investigation. Without more, Defendant has not shown how the software, source code, manuals, and validation testing information requested by Defendant would be helpful in raising reasonable doubt.

(b) Materiality based on the Government's case-in-chief

Defendant contends the use of Torrential Downpour to access Defendant's computer is "directly at issue" because the Government "will presumably" present evidence in its case-in-chief of the investigation of the charges.[136] The Government does not expressly respond to this argument.

While it is reasonable to predict that the Government will present testimony regarding Detective Baine's use of Torrential Downpour during the December 2012 on-line investigation, Ms. Bush's declaration does not elucidate how the requested information would assist Defendant's response to the Government's case-in-chief. Without more, Defendant has not demonstrated the materiality of the requested information based on the Government's presentation of evidence regarding the on-line investigation during its case-in-chief.[137]

[136] Def.'s mot. to compel at 3.

[137] Federal Rule of Criminal Procedure 16 has a separate provision for the disclosure of any item "the government intends to use . . . in its case-in-chief at trial." Fed. R. Cr. P. 16(a)(1)(E)(ii). Neither party cites or

(c) Materiality for cross-examination of Detective Baine

Defendant asserts the requested information is needed to "adequately prepare for the cross-examination of Detective Baine."[138] The Government does not expressly respond to this argument.

While it is likely that a trial would include the Government's presentation of Detective Baine as a witness, there is no showing of record that Detective Baine is or should be knowledgeable about Torrential Downpour's software functionality, source code, or validation testing. An investigator using law enforcement software can testify to "how he interfaced with the [software] and what resulted from his efforts" and "does not have to know about or explain how the [software] program executes its source code; he just has to describe the manner in which he used it." United States v. Blouin, CR16-307 TSZ, 2017 WL 3485736, at *6 (W.D. Wash. Aug. 15, 2017).

Nor does Defendant address in what specific manner his access to the Torrential Downpour user manual would assist him in preparing for the cross-examination of Detective Baine regarding his use of Torrential Downpour in December 2012 where, as here, the Government has provided a demonstration of a simulated investigation using the version of Torrential Downpour used by Detective Baine.[139] Nothing in the material submitted by

discusses this Rule in support of its position regarding the materiality of or the Court's consideration of the disclosure of the requested information.

[138] Def.'s mot. to compel at 7, 8-9.

[139] Defendant urges the decision in Chiaradio supports the disclosure of the Torrential Downpour manuals because the defendant in Chiaradio received a recording of the transfer occurring during the on-line investigation as well as manuals about how to reconstruct the download in the manner used by law enforcement. United States v. Chiaradio, 684 F.3d 265, 277 (1st Cir. 2012). The Court disagrees. During the hearing, Defendant received the log relating to Detective Baine's on-line investigation, a Powerpoint presentation about the installation and use of uTorrent version 2.2.1, and a compact disc presentation of a simulation of how law enforcement personnel use Torrential Downpour, with Detective Erdely providing further explanation of each item.

Defendant, specifically Ms. Bush's declaration, supports a conclusion that any of the requested information is necessary to enable an effective cross-examination of Detective Baine.

(d) Materiality for search warrant challenge

Defendant contends he needs the source code, software, manuals, and validation testing information relating to Torrential Downpour because use of Torrential Downpour is the sole basis of the search warrant. Without the requested information, Defendant asserts, his attorney cannot adequately analyze whether the software was functioning correctly or whether the preliminary on-line search and subsequent downloads of "potential evidence" violated the Fourth Amendment, comported with information in the search warrant, or constituted a form of computer hacking. The Government counters that its access to a defendant's computer through information the computer makes publicly available through a file-sharing network and file-sharing software is not a violation of the Fourth Amendment. Here, the Government urges Defendant has not demonstrated any manner in which the Government accessed the files on Defendant's computer during the December 2012 on-line investigation other than through publicly available information provided by Defendant's computer.

To the extent the Court may properly address Rule 16 materiality in the context of a challenge to a search warrant,[140] Defendant does not specify in what way the on-line search and downloads arguably (1) violated the Fourth Amendment, (2) failed to comport with information in the search warrant, or (3) constituted hacking. Nor does Defendant point out the aspects of his expert's declaration that support his request for information based on a search warrant challenge. Without more, Defendant has not satisfactorily demonstrated the materiality of the requested information to any challenge to the search warrant.

[140] See United States v. Soto-Zuniga, 837 F.3d 992, 1000-01 (9th Cir. 2016) (finding Armstrong, supra, is limited to claims of selective prosecution and does not "preclude Rule 16(a)(1)(E) discovery related to the constitutionality of a search or seizure").

A recent decision of the district court for the Eastern District of Wisconsin is instructive with respect to Defendant's motion to compel on this ground. See United States v. Feldman, No. 13-CR-155, 2014 WL 7653617, at *3-7 (E.D. Wis. July 7, 2014), upheld as without clear error in United States v. Feldman, No. 13-CR-155, 2015 WL 248006, at *6-7 (E.D. Wis. Jan. 19, 2015). In Feldman, the Government charged the defendant with receipt and possession of child pornography after conducting an on-line investigation of a peer-to-peer file sharing network. Feldman, 2014 WL 7653617, at *1. The court clarified that the law enforcement software "was the means by which law enforcement identified [the defendant] as a suspect and established the basis for the search warrant [but t]he charges against [the defendant] stem[med] from what was recovered from [the defendant's] home pursuant to th[e] search warrant." Id. The court distinguished Budziak because there the defendant was charged with distributing child pornography "related to conduct that occurred over the peer-to-peer network." Id. at 5. In Feldman, the court concluded, the defendant was "not charged with any conduct that law enforcement observed via" use of the law enforcement software.[141] Id.

Characterizing the defendant's request for the law enforcement software program, manual, protocols and technical specifications as "most plausibly . . . relevant to an effort to challenge the search warrant," the court in Feldman decided that the defendant had not demonstrated how the requested information was relevant to a search warrant challenge. Id. Specifically, the court found the defendant did not "adequately support his speculation that [the law enforcement software] may be capable of intruding into private portions of a target computer, [and] even if true, the defendant offer[ed] no indication as to how this might

[141] Because the charges arose out of material investigators found in the defendant's home, rather than out of "conduct the investigator observed over the peer-to-peer network," the court in Feldman characterized both the law enforcement software and the investigator using that software as not "'transactional witnesses' to the offense charged." Feldman, 2014 WL 7653617, at *1.

undermine the search warrant obtained for his residence." Id. The court noted there was no suggestion that information in the affidavit supporting the search warrant was

> obtained by any sort of intrusion or how any sort of information obtained through an intrusion might be used against him at trial. . . . Information obtained without intruding upon [the private or non-shared space of the defendant's computer], e.g. the hash value matches and the defendant's IP address, . . . the facts crucial to the establishment of probable cause in this case, would not be subject to suppression.

Id.[142]

This case presents factual circumstances nearly identical to those in Feldman. The Government charged Defendant with receipt and possession of child pornography after an on-line investigation of a peer-to-peer file-sharing network. Detective Baine and Detective Partney used Torrential Downpour to identify Defendant's computer and as the basis for a search warrant.[143] Yet it appears that the pending charges are not based on any files discovered or downloaded during Detective Baine's on-line investigation. As discussed earlier, the absence of any reference to a downloaded file in the superseding indictment supports a conclusion the pending charges are not based on the use of Torrential Downpour during the on-line investigation. Instead, the available record suggests that the charges pending against Defendant are based on images and videos discovered on items seized from Defendant's home several months after the on-line investigation occurred.

[142] The court also rejected the defendant's contention that the distinctions between the law enforcement software and an "ordinary consumer version of peer-to-peer network file sharing software" supports disclosure of the requested information. Feldman, 2014 WL 7653617, at *6. The court reasoned that the Government used the law enforcement software "not to peer into a suspect's home . . . but to monitor [the defendant]'s activities on a public peer-to-peer network, a space where [the defendant] had no reasonable expectation of privacy." Id.

[143] Detective Partney's affidavit in support of the search warrant listed as child pornography two files beginning with the phrase "spread.em.chan." That phrase is at the beginning of each file reported as downloaded from Defendant's computer by the log of activity occurring during Detective Baine's December 2012 on-line investigation.

Unlike the circumstances in Feldman, however, Defendant presents, through his expert's declaration, concerns that Torrential Downpour may have visited private or non-shared parts of Defendant's computer during the December 2012 on-line investigation. Ms. Bush's concern is based on: (1) her experience with other investigations in which she reportedly examined seized computers and (2) the reported results of the Government's forensic examination of the seized items. In particular, Ms. Bush declares that the forensic report did not reveal information either that the files downloaded by Detective Baine were found or that a large part of the discovered child pornography was available in public areas of Defendant's computer. Yet, Ms. Bush's concern is not based on her examination of the uTorrent software used by Defendant's computer to access the BitTorrent network, despite the fact the forensic report available of record states that software was located on one of the seized items. Nor is Ms. Bush's concern based on her examination of any of the items seized from Defendant's home, including any device Detective Baine connected to during his on-line investigation. At this point, the record does not support a concern that the files downloaded during the December 2012 on-line investigation, which are referenced in the affidavit supporting the search warrant, were obtained by Torrential Downpour accessing non-public parts of Defendant's computer.[144]

While a Fourth Amendment challenge may arise out of the government's search of a location over which a person has a legitimate expectation of privacy, "a person has no legitimate expectation of privacy in information [the person] voluntarily turns over to third parties." Smith v. Maryland, 442 U.S. 735, 739-40, 743-44 (1979) (finding the installation and use of a pen

[144] Defendant questions, "how do we know that the single source download is not accessing encrypted portions of a suspect machine in the manner Ms. Bush's affidavit raises?" Def't post-hr'g mem. at 13. Defendant does not, however, explain the "manner" of access to encrypted information reportedly "raise[d]" in Ms. Bush's declaration. Nor does Ms. Bush's declaration provide a description of the manner in which the access may have occurred. Rather, Ms. Bush asserts that such access may have occurred based on her experience with other investigations and the absence from the forensic report of information she considers pertinent to the issue.

register did not constitute a search because the defendant had no legitimate expectation of privacy in telephone numbers he dialed). With regard to law enforcement access to a person's computer, the Eighth Circuit has held that a defendant has "no reasonable expectation of privacy in files that [law enforcement] retrieved from [a defendant's] personal computer where [the defendant] installed and used [file-sharing software] to make his files accessible to others." United States v. Stults, 575 F.3d 834, 843 (8th Cir. 2009).[145] While Defendant may challenge a search based on law enforcement's access to non-public information, Ms. Bush's declaration is not sufficient to support a conclusion such a challenge is reasonable here.

To the extent Defendant relies on Budziak to support this ground for disclosure, the case is distinguishable. The Ninth Circuit found that the defendant "submitted evidence suggesting that the FBI agents could have used the [law enforcement] software to override [the defendant's] sharing settings." Budziak, 697 F.3d at 1112. Here, the Court finds Ms. Bush's declaration insufficient to support a suggestion that Detective Baine's on-line investigation accessed non-shared information on Defendant's computer. Without more, neither the expert's experience with other investigations nor the expert's critique of the Government's forensic report in the absence of the expert's own examination of the seized items is sufficient to establish the materiality of the requested information for purposes of challenging the search warrant. See Feldman, supra. Under the circumstances, Defendant has not established how the requested information is material under Rule 16(a)(1)(E)(i), or helpful to his defense. See also United States v. Maurek, No. CR-15-129-D, 2015 WL 12915605, at *3 (W.D. Okla. Aug. 31, 2015)

[145] The Eighth Circuit recently distinguished law enforcement's access to information from an individual's personal computer gained by the computer's participation in public file sharing from law enforcement's access to information from an individual's computer gained by law enforcement "sen[ding] computer code . . . that searched [the computer] for specific information and sent that information back to law enforcement." United States v. Horton, 863 F.3d 1041, 1047 (8th Cir. 2017) (addressing law enforcement's use of a Network Investigative Technique ("NIT")). Nothing of record shows law enforcement obtained information about Defendant's computer other than through information the computer made publicly available through file-sharing.

(denying motion to compel discovery of Torrential Downpour software due to the defendant's failure "to make a threshold showing of materiality").

B. Law enforcement privilege

The Government also argues that the requested information is protected from disclosure by a privilege protecting sensitive law enforcement investigation techniques.[146] Noting that it has the initial burden to demonstrate the privilege applies to the requested materials, the Government states that, if it satisfies its burden, a court then engages in a balancing test to ascertain whether or not to require disclosure. In support of its position that the privilege applies to preclude disclosure of the information requested by Defendant, the Government relies on the First Circuit's decision in Chiaradio, supra, as "strongly impl[ying] that the privilege would operate to bar discovery" of the source code of a law enforcement investigative software program.[147] The Government also relies on the affidavit and testimony of Detective Erdely regarding the sensitive nature of the requested information and the need to protect the requested information from disclosure to protect law enforcement investigations.

Defendant does not dispute that the privilege may apply to requests for sensitive law enforcement techniques. Instead, Defendant argues that the Government did not adequately demonstrate a basis for application of the privilege in this case. Defendant further urges that the balancing of factors requires disclosure under the circumstances of this case. Specifically, Defendant asserts the requested Torrential Downpour information "go[es] directly to the critical

[146] Gov't Response to Def.'s mot. compel at 22-26; Gov't's post-hr'g mem. at 11-13.

[147] Gov't Response to Def.'s mot. compel at 23. The Government also cites to two cases addressing the qualified law enforcement privilege in contexts other than the request of a defendant in a pending criminal case: In re Department of Investigation of the City of N.Y. v. Myerson, 856 F.2d 481, 484 (2nd Cir. 1988) and Commonwealth of Puerto Rio v. United States, 490 F.3d 50 (1st Cir. 2007). The Court need not further address these decisions because courts have addressed the privilege in the context of a request by a defendant in a criminal case.

issues surrounding both the search warrant and Count I," and is necessary to adequately prepare for the cross-examination of Detective Baine.[148] Defendant also contends a court order granting Defendant's motion to compel discovery could include "appropriate protective measures that would limit the conditions under which [the requested] Torrential Downpour [information] is reviewed."[149] Defendant presents no evidence beyond his expert's declaration to support his position with regard to application of the qualified law enforcement privilege.

1. *Standard for qualified law enforcement privilege*

A litigant asserting the law enforcement privilege has the burden to establish the privilege applies to the information in question. In re The City of N.Y., 607 F.3d 923, 944, 948 (2nd Cir. 2010); accord United States v. Matish, 193 F. Supp. 3d 585, 597 (E.D. Va. 2016); United States v. Briggs, 831 F. Supp.2d 623, 630 (W.D. N. Y. 2011). After a litigant shows the privilege applies, a court engages in a balancing process to decide whether the litigant's need for access to the privileged information outweighs the public's interest in nondisclosure. In re The City of N.Y.¸ 607 F.3d at 945, 948; Matish, 193 F. Supp.3d at 597-98. As the Eighth Circuit stated when addressing a state court's refusal to disclose the identity of a confidential informant in the context of a state habeas proceeding, "the decision to order disclosure varies with the particular circumstances of each case." Barnes v. Dormire, 251 F.3d 767, 770 (8th Cir. 2001) (citing Roviaro v. United States, 353 U.S. 53, 62 (1957)).

Courts have applied the privilege to protect from disclosure: (1) "the nature and location of electronic surveillance equipment," United States v. Van Horn, 789 F.2d 1492, 1507-08 (11th

[148] Def.'s mot. compel at 6-7.

[149] Def.'s mot. compel at 11; see also Def.'s post-hr'g mem. at 17-19.

Cir. 1986),[150] as well as (2) "user manuals, test data, and related software" pertaining to a mobile tracking device used by investigators to locate an aircard, United States v. Rigmaiden, 844 F. Supp.2d 982, 1002 (D. Ariz. 2012). Application of the privilege is proper if disclosure "will educate criminals regarding how to protect themselves against police surveillance," Van Horn, 789 F.2d at 1508, or "would hamper future law enforcement efforts by enabling adversaries of law enforcement to evade detection," Rigmaiden, 844 F. Supp.2d at 1002.

2. *Application of the privilege*

In support of its position, the Government relies on the sworn statements of Detective Erdely providing that: (1) the requested source code, program, and investigated infohashes, as well as the version of software law enforcement personnel appear as during an on-line investigation, are "extremely confidential and law enforcement sensitive";[151] (2) disclosure of the requested information would expose and make available to the public the child pornography torrents investigated by law enforcement, as well as the hash values of investigated files;[152] and (3) with the requested information, individuals could make changes to thwart or avoid law enforcement investigations of child pornography available on-line.[153] Additionally, Detective Erdely explained the Torrential Downpour manuals contain information about law enforcement's

[150] Accord United States v. Cintolo, 818 F.2d 980, 1002-03 (1st Cir. 1987) (affirming a district court's refusal to allow cross-examination about "the precise location of the electronic surveillance devices hidden in [an] apartment" based on the government's objection that information about the location of the surveillance devices "would jeopardize future criminal investigations"). The First Circuit applied the law enforcement privilege because "discoverability of this kind of information will enable criminals to frustrate future government surveillance and perhaps unduly jeopardize the security of ongoing investigations" and the defendant had not sufficiently demonstrated a need for the information. Id.

[151] Hr'g Tr. at 115.

[152] Hr'g Tr. at 156-57.

[153] Hr'g Tr. at 156-57.

server, its location, and how law enforcement accesses it.[154] These statements establish that disclosure of the requested information would hamper future and ongoing law enforcement efforts by enabling those individuals obtaining child pornography on- line to evade detection. The Government has satisfied its burden of demonstrating the basis for application of the law enforcement privilege to the Torrential Downpour material requested by Defendant.

Defendant has not sufficiently established a need for the privileged information sufficient to overcome the privilege. Defendant relies solely on his expert's declaration. The declaration does not support a conclusion that Defendant's need for the requested information outweighs the public's interest in non-disclosure.

C. <u>Defendant's alternative request for disclosure under Rule 17(c)</u>

In the "Wherefore" paragraph of his post-hearing brief, Defendant asks the Court to treat Defendant's motion to compel discovery under Rule 16 as a request for a subpoena under Federal Rule of Criminal Procedure 17(c). The Government opposes Defendant's Rule 17(c) request as not the proper subject of discovery in a criminal case, citing <u>United States v. Bueno</u>, 443 F.3d 1017, 1026 (8th Cir. 2006) (citing <u>United States v. Nixon</u>, 418 U.S. 683, 698-99 (1974)).

Rule 17(c) provides in relevant part that:

> [a] subpoena may order [a] witness to produce any books, papers, documents, data, or other objects the subpoena designates. The court may direct the witness to produce the designated items in court before the trial or before they are to be offered in evidence. When the items arrive, the court may permit the parties and their attorneys to inspect all or part of them.

Fed. R. Cr. P. 17(c)(1). To uphold a pretrial subpoena under Rule 17(c) a court must consider a variety of factors other than materiality of the subpoenaed materials to the Defendant's defense.

[154] Hr'g Tr. at 75.

See, e.g., Nixon, 418 U.S. at 699-700; United States v. Hardy, 224 F.3d 752, 755-56 (8th Cir. 2000). To the extent the Court may consider Defendant's motion to compel discovery as a motion for a Rule 17(c)(1) subpoena, Defendant has not adequately addressed the factors relevant to a court's consideration of such a subpoena. Therefore, the Court denies this request without prejudice.

Conclusion

Accordingly, after careful consideration,

IT IS HEREBY ORDERED that Defendant's motion to compel discovery [ECF No. 27] is **DENIED without prejudice** to the extent Defendant relies on the Supreme Court decisions in Brady and Giglio.

IT IS FURTHER ORDERED that Defendant's motion to compel discovery [ECF No. 27] is **DENIED without prejudice** to the extent Defendant seeks relief under Federal Rule of Criminal Procedure 17(c).

IT IS FINALLY ORDERED that Defendant's motion to compel discovery [ECF No. 27] is otherwise **DENIED**.

Patricia L. Cohen

PATRICIA L. COHEN
UNITED STATES MAGISTRATE JUDGE

Dated this 25th day of August, 2017.